

Администрирование сетевых подсистем

Лабораторная работа №15

Авдадаев Джамал Геланиевич

15 декабря 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Получить практические навыки настройки сетевого журналирования с использованием rsyslog на сервере и клиенте.

Настройка сервера rsyslog



Рис. 1: Конфигурация netlog-server.conf

Включение TCP-приёма сообщений

```
>client.dgavdadaev.net:43644 (ESTABLISHED)
rsyslogd 14826 root 4u IPv4 59870 0t0 TCP *:shell (LISTEN)
rsyslogd 14826 root 5u IPv6 59871 0t0 TCP *:shell (LISTEN)
rsyslogd 14826 14829 in:imjour root 4u IPv4 59870 0t0 TCP *:shell (LISTEN)
rsyslogd 14826 14829 in:imjour root 5u IPv6 59871 0t0 TCP *:shell (LISTEN)
rsyslogd 14826 14830 in:imtcp root 4u IPv4 59870 0t0 TCP *:shell (LISTEN)
rsyslogd 14826 14830 in:imtcp root 5u IPv6 59871 0t0 TCP *:shell (LISTEN)
rsyslogd 14826 14831 w0/imtcp root 4u IPv4 59870 0t0 TCP *:shell (LISTEN)
rsyslogd 14826 14831 w0/imtcp root 5u IPv6 59871 0t0 TCP *:shell (LISTEN)
rsyslogd 14826 14832 w1/imtcp root 4u IPv4 59870 0t0 TCP *:shell (LISTEN)
rsyslogd 14826 14832 w1/imtcp root 5u IPv6 59871 0t0 TCP *:shell (LISTEN)
rsyslogd 14826 14833 rs:main root 4u IPv4 59870 0t0 TCP *:shell (LISTEN)
rsyslogd 14826 14833 rs:main root 5u IPv6 59871 0t0 TCP *:shell (LISTEN)
[root@server.dgavdadaev.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.dgavdadaev.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
[root@server.dgavdadaev.net rsyslog.d]#
```

Рис. 2: Проверка портов rsyslog

Настройка клиента rsyslog



Рис. 3: netlog-client.conf

Просмотр журналов

Проверка получения логов сервером

```
Dec 11 11:04:12 server systemd[1]: systemd-coredump@81-13750-0.service: Deactivated successfully.
Dec 11 11:04:16 client kernel: traps: VBoxClient[13749] trap int3 ip:41dd1b sp:7f3ac9977cd0 error:0 in VBoxClient[1dd1b,400000+bb000]
Dec 11 11:04:16 client systemd-coredump[13750]: Process 13746 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, process
ing...
Dec 11 11:04:16 client systemd[1]: Started systemd-coredump@81-13750-0.service - Process Core Dump (PID 13750/UID 0).
Dec 11 11:04:16 client systemd-coredump[13751]: Process 13746 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from rpm l
ibXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10
.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#
012Stack trace of thread 13749:#012#0 0x00000000041dd1b n/a (n/a + 0x0)#012#1 0x000000000041dc94 n/a (n/a + 0x0)#012#2 0x000000000045
041c n/a (n/a + 0x0)#012#3 0x0000000004355d0 n/a (n/a + 0x0)#012#4 0x000007f3ad801eb68 start_thread (libc.so.6 + 0x94b68)#012#5 0x0000
7f3ad808f6bc __clone3 (libc.so.6 + 0x1056bc)#012#012Stack trace of thread 13746:#012#0 0x000007f3ad808d4bd syscall (libc.so.6 + 0x1034bd)
#012#1 0x00000000004344e2 n/a (n/a + 0x0)#012#2 0x0000000000450066 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x0
0007f3ad7fb430e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x000007f3ad7fb43c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9
)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Dec 11 11:04:16 client systemd[1]: systemd-coredump@81-13750-0.service: Deactivated successfully.
Dec 11 11:04:17 server systemd[1]: serial-getty@ttyS0.service: Deactivated successfully.
Dec 11 11:04:17 server systemd[14337]: Created slice background.slice - User Background Tasks Slice.
Dec 11 11:04:17 server systemd[14337]: Starting systemd-tmpfiles-clean.service - Cleanup of User's Temporary Files and Directories
```

Рис. 4: Входящие сообщения в messages

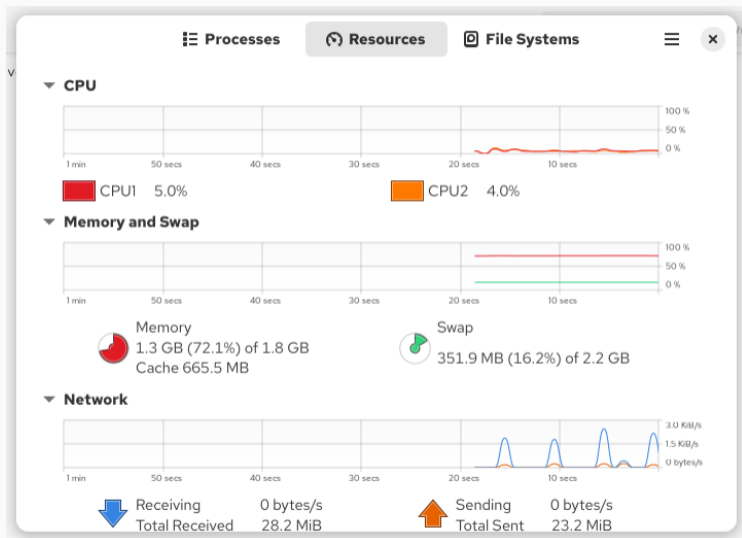


Рис. 5: gnome-system-monitor

Установка консольного просмотрщика

```
[root@server.dgavdadaev.net ~]# dnf -y install lnav
Extra Packages for Enterprise Linux 10 - x86_64
Extra Packages for Enterprise Linux 10 - x86_64
Rocky Linux 10 - BaseOS
Rocky Linux 10 - BaseOS
Rocky Linux 10 - AppStream
Rocky Linux 10 - AppStream
Rocky Linux 10 - CRB
Rocky Linux 10 - CRB
Rocky Linux 10 - Extras
Rocky Linux 10 - Extras
No match for argument: lnav
Error: Unable to find a match: lnav
[root@server.dgavdadaev.net ~]#
```

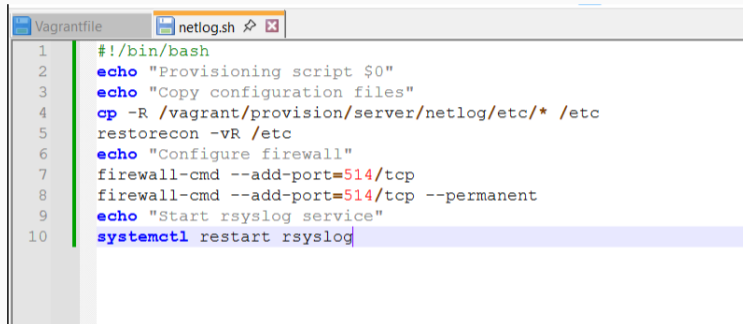
21 kB/s		34 kB	00:01
12 MB/s		5.6 MB	00:00
11 kB/s		4.3 kB	00:00
11 MB/s		4.1 MB	00:00
12 kB/s		4.3 kB	00:00
2.0 MB/s		2.0 MB	00:01
14 kB/s		4.3 kB	00:00
952 kB/s		484 kB	00:00
7.4 kB/s		3.1 kB	00:00
12 kB/s		4.8 kB	00:00

Рис. 6: Ошибка установки lnav

Автоконфигурация Vagrant: сервер

```
[root@server.dgavdadaev.net rsyslog.d]#  
[root@server.dgavdadaev.net rsyslog.d]# cd /vagrant/provision/server/  
[root@server.dgavdadaev.net server]# mkdir -p /vagrant/provision/server/netlog/etc/rsyslog.d  
[root@server.dgavdadaev.net server]# cp -R /etc/rsyslog.d/netlog-server.conf /vagrant/provision/server/netlog/etc/rsyslog.d/  
[root@server.dgavdadaev.net server]# touch netlog.sh  
[root@server.dgavdadaev.net server]# █
```

Рис. 7: Создание структуры provisioning



The image shows a code editor window with two tabs: 'Vagrantfile' and 'netlog.sh'. The 'netlog.sh' tab is active, displaying a shell script. The script starts with a shebang line, followed by echo statements for provisioning and file copying. It then uses 'cp' to copy files from a Vagrant provision directory to the server's /etc directory, followed by 'restorecon' to restore SELinux context. Next, it echoes a message about firewall configuration and uses 'firewall-cmd' to add port 514/tcp twice, once without the --permanent flag and once with it. Finally, it echoes a message about starting rsyslog and uses 'systemctl' to restart the service. Line numbers 1 through 10 are visible on the left side of the editor.

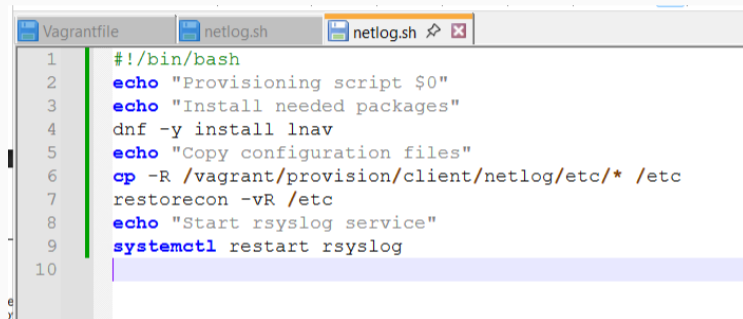
```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Copy configuration files"
4  cp -R /vagrant/provision/server/netlog/etc/* /etc
5  restorecon -vR /etc
6  echo "Configure firewall"
7  firewall-cmd --add-port=514/tcp
8  firewall-cmd --add-port=514/tcp --permanent
9  echo "Start rsyslog service"
10 systemctl restart rsyslog
```

Рис. 8: Скрипт netlog.sh (server)

Автоконфигурация Vagrant: клиент

```
-----  
[root@client.dgavdadaev.net rsyslog.d]#  
[root@client.dgavdadaev.net rsyslog.d]# cd /vagrant/provision/client/netlog/etc/rsyslog.d  
-bash: cd: /vagrant/provision/client/netlog/etc/rsyslog.d: No such file or directory  
[root@client.dgavdadaev.net rsyslog.d]# mkdir -p /vagrant/provision/client/netlog/etc/rsyslog.d  
[root@client.dgavdadaev.net rsyslog.d]# cd /vagrant/provision/client/  
[root@client.dgavdadaev.net client]# cp -R /etc/rsyslog.d/netlog-client.conf /vagrant/provision/c  
netlog/etc/rsyslog.d/  
[root@client.dgavdadaev.net client]# touch netlog.sh  
[root@client.dgavdadaev.net client]# █
```

Рис. 9: Экспорт client netlog



The image shows a terminal window with three tabs: 'Vagrantfile', 'netlog.sh', and 'netlog.sh' (highlighted). The terminal displays a shell script with line numbers 1 through 10. The script uses 'echo' for messages, 'dnf' for package installation, 'cp' for file copying, and 'systemctl' for service management.

```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Install needed packages"
4  dnf -y install lnav
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/client/netlog/etc/* /etc
7  restorecon -vR /etc
8  echo "Start rsyslog service"
9  systemctl restart rsyslog
10
```

Рис. 10: Скрипт netlog.sh (client)

Выводы

- Настроены сервер и клиент rsyslog для сетевого журналирования.
- Обеспечена передача сообщений по TCP-порту 514.
- Реализованы provisioning-скрипты для автоматизации развёртывания.
- Проверена работа логирования и взаимодействие journald ↔ rsyslog.
- Лабораторный стенд полностью функционирует и соответствует заданию.